

Research Article

An Optimized Approach for Secure Data Transmission Using Spread Spectrum Audio Steganography, Chaos Theory, and Social Impact Theory Optimizer

Rohit Tanwar ^(D),¹ Kulvinder Singh,² Mazdak Zamani ^(D),³ Amit Verma,¹ and Prashant Kumar¹

¹University of Petroleum and Energy Studies, Dehradun, India ²UIET Kurukshetra University, Kurukshetra, India ³Felician University, Lodi, New Jersey, USA

Correspondence should be addressed to Rohit Tanwar; rohit.tanwar.cse@gmail.com

Received 9 April 2019; Revised 10 July 2019; Accepted 29 July 2019; Published 8 September 2019

Academic Editor: Liansheng Tan

Copyright © 2019 Rohit Tanwar et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

Being easy to understand and simple to implement, substitution technique of performing steganography has gain wide popularity among users as well as attackers. Steganography is categorized into different types based on the carrier file being used for embedding data. The audio file is focused on hiding data in this paper. Human has associated an acute degree of sensitivity to additive random noise. An individual is able to detect noise in an audio file as low as one part in 10 million. Given this limitation, it seems that concealing information within audio files would be a pointless exercise. Human auditory system (HAS) experiences an interesting behavior known as masking effect, which says that the threshold of hearing of one type of sound is affected by the presence of another type of sound. Because of this property, it is possible to hide some data inside an audio file without being noticed. In this paper, the research problem for optimizing the audio steganography technique is laid down. In the end, a methodology is proposed that effectively resolves the stated research problem and finally the implementation results are analyzed to ensure the effectiveness of the given solution.

1. Introduction

Currently, audio steganography is limited to providing solutions related to copyright and assurance of the integrity of content [1]. It is possible to expand its applications to incorporate the embedding of covert communications as well. Various audio steganography strategies are developed and utilized for embedding knowledge in audio files. These strategies embrace low-bit encoding (LSB), polarity inversion, echo activity, part committal to writing, cepstral activity, sensory activity masking, and spread spectrum [2, 3]. Low-bit encoding (LSB) is the most famous technique, but it suffers from some severe limitations. Out of other techniques of communication, spread spectrum is receiving increasing attention. Spread spectrum technology forms the premise of spread spectrum steganography [4–7]. Because of the higher data hiding capacity of the low-bit encoding substitution technique, its alternate is expected to have similar capacity while maintaining better robustness and imperceptibility. Therefore, there is a requirement for incorporating optimization technique with a steganography method so that the required expectations can be fulfilled effectively [8–12].

2. Motivation and Scope for Optimization

The effectiveness of a steganography technique is analyzed on the parameters, namely, capacity, imperceptibility, and robustness. In most of the existing techniques, adherence with one of these parameters is usually achieved at the cost of comprising with other parameters. Low-bit encoding or LSB technique is the most commonly used technique [13–19]. However, the inherent limitations of the LSB method that are listed below inspire to look for an effective and optimized alternate approach [20–24]:

- (i) LSB method is prone to intentional attacks as data are embedded in LSBs only
- (ii) Unintentional attacks like noise disturbances are the cause of data loss

The literature relevant to audio steganography techniques was studied [25–49], and the observations are summarized as a comparison of the techniques on the basic parameters, like robustness, imperceptibility, capacity, and complexity, as shown in Table 1. The analysis says that it is difficult for an existing technique to achieve the satisfactory value of all the comparison parameters. A method that yields high capacity does not have adequate robustness and imperceptibility. Similarly, if robustness was there, the capacity is compromised. Therefore, an audio steganography technique needs to be optimized so that the acceptable values of evaluation parameters are achieved.

3. Problem Formulation

The objective is to design an optimized method that should be having a capacity similar to the LSB technique, but robustness should be high, unlike the LSB method. However, there is always a tradeoff in achieving capacity along with keeping the high value of robustness. Thus, the research problem is stated using the following points:

- (i) An audio steganography technique is desired that should have the capacity comparable to the LSB technique but maintaining a high value of robustness and imperceptibility.
- (ii) Most of the techniques of implementing audio steganography that possesses satisfactory robustness have less hiding capacity. Therefore, the selected technique is customized to meet the requirements.
- (iii) As a consequence of the customization for high capacity, more distortion will get induced in the cover file after embedding. To minimize that distortion, an optimization algorithm is used in coordination with the embedding algorithm.
- (iv) The sequence of embedding message bits in the audio file should not be obvious. The embedding pattern is expected to be as less predictable as possible to make the technique more secure.

4. Proposed Methodology

The proposed methodology resolves the research problem in an efficient manner. A coordinated approach using spread spectrum steganography, SITO, and chaos theory works in a way that the objectives of the research problem are satisfied. The underlying representation of the proposed method is shown in Figure 1.

The proposed method comprised the following basic modules:

TABLE 1: Comparison of audio steganography techniques.

| Techniques | Parameters | | | |
|--------------------|------------------|----------|------------|------------|
| | Imperceptibility | Capacity | Robustness | Complexity |
| LSB | Medium | High | Low | Low |
| Parity coding | Medium | Medium | Low | Low |
| Phase coding | High | Low | High | Medium |
| Spread spectrum | Low | Medium | High | High |
| Echo hiding | Low | Medium | Medium | Medium |
| Tone insertion | Low | Low | Medium | High |

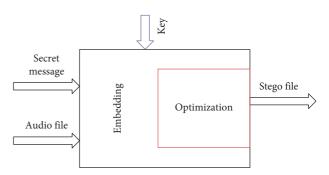


FIGURE 1: Proposed solution representation.

- (i) Chaotic system: chaotic map is used to provide required randomness as the pseudorandom numbers generated through some random library function result in a repetition of some pattern to be used for substitution. The cross correlation between two consecutive numbers generated through chaotic map approaches to zero. The key is obtained using logistic maps of chaos theory.
- (i) Spread spectrum: spread spectrum technique of implementing audio steganography is used as one of the prime components of the proposed solution. Because of its inherent robustness, difficult to intercept, and hard to interference, the technique is the first choice in solving the given research problem.
- (ii) Social impact theory optimization: to minimize the distortion induced in audio samples because of embedding, social impact theory optimization (SITO) is used. In recent researches, SITO has outperformed genetic algorithm (GA) and particle swarm optimization (PSO) in achieving optimum results. The algorithm evolves iteration by iteration based on some objective functions and guarantees a nearly optimal solution at the end. The stopping criterion for the algorithm in the current research is the number of iterations.

4.1. *Proposed Algorithm.* The methodology starts with a capacity check operation to verify the capability of the chosen cover audio file to embed the secret message of given

```
Step 1: procedure Embed_Optimize(aud_file, img_file)
Step 2: if(capacity_check(aud_file, img_file) = TRUE) then
Step 3: Temp_aud←transform(aud_file)
           Temp_img←Binary(img_file)
Step 4:
Step 5:
           seed←random()
Step 6:
           kev←seed
Step 7:
           count←0
Step 8:
           while no_of_iteration \leq 100 do
Step 9:
             if count < length(Temp_img) then
Step 10:
                key←SITO_OPT(key)
Step 11:
              hide(Temp_aud, key, Temp_img)
Step 12:
                count←update(count)
Step 13:
              else
Step 14:
                Write"Message got embedded successfully".
Step 15:
            repeat
            return Temp_aud
Step 16:
Step 17:
            else
Step 18:
            exit()
Step 19:
            return
```

ALGORITHM 1: Optim_Audio, input: Audio file, image file, output: stego file.

size successfully. After that, the cover audio file is transformed into its equivalent spread spectrum. Simultaneously, the secret message is converted into its binary equivalent. The required random sequence that acts as a key to guide the spreading of message bits over the entire spectrum of the cover file is obtained using the logistic map of chaotic theory. The embedding step is repeated until the complete message is hidden inside the cover file. The amount of data that is embedded per sample of the audio file is comparatively more so that capacity is increased. The initial values are calculated for evaluation parameters as well as the objective function. The proposed algorithm is given in Algorithm 1.

In order to optimize the value of the objective function, SITO is used. The values of evaluation parameters are improved with the iterations of the optimization algorithm. The SITO terminates when an acceptable value of evaluation parameters is achieved or the number of iterations is over. The flow chart given in Figure 2 describes the proposed methodology.

4.1.1. Objective Function. The objective is to minimize MSE and maximize PSNR and SSIM. The aggregate function used here is a minimizing function given as

$$f: \min\left[\frac{\text{MSE}}{\text{PSNR} \times \text{SSIM}}\right], \tag{1}$$

where MSE stands for mean square error, PSNR stands for peak signal to noise ratio, and SSIM stands for structural similarity index.

5. Implementation

MATLAB is a multiparadigm environment developed for numerical computing primarily. With time, it got equipped with a list of toolboxes developed for specific needs. Initially, the command window was the only way to interact for executing files. Later, an additional feature of graphical interface benefitted the users. Because of its broad applicability, popularity, and effectiveness, the proposed algorithm is implemented using MATLAB. The open-source libraries are used for implementing chaos theory and SITO. To compare and analyze the effectiveness of the proposed algorithm, the comparison graphs are generated for PSNR, MSE, and SSIM. MATLAB 2014 is used as the simulation environment. The details regarding secret message embedded, cover audio file, and libraries used are given in the following:

- (i) Secret message: (i) JPG image of size 8.78 KB and dimension 244 × 250; (ii) PNG image of size 38.6 KB and dimension 512 × 512
- (ii) Cover audio: MP4 file of size 5.07 MB and length 3 min 21 sec, bit rate 206 kbps, channels 2, and audio sample rate 44.100 kHz
- (iii) CODO library: library used for random number generator using chaos theory
- (iv) SITO library: library used for optimizer using social impact theory

6. Result Analysis

The effectiveness of the proposed solution of the formulated problem is evaluated through the following methods:

- (i) Histogram analysis of original message and extracted message
- (ii) Frequency spectrum analysis of cover audio and stego audio
- (iii) Peak signal to noise ratio (PSNR)
- (iv) Mean square error (MSE)
- (v) Structural similarity index (SSIM)
- (vi) Visual inspection of the original message and extracted message

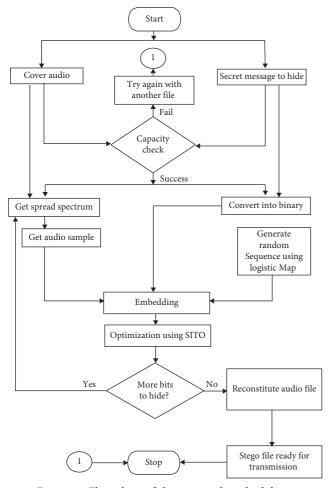


FIGURE 2: Flow chart of the proposed methodology.

- (vii) Robustness measurement using correlation coefficient
- (viii) Comparison of variation of PSNR, MSE, and SSIM with some existing techniques

6.1. Histogram of Original Image and Extracted Image. An image is taken as secret data to be embedded in audio. Histogram representation of an image is a popular way of analyzing images.

Either the histograms can be taken of the single channel out of RGB or it can be taken of RGB in aggregate. The given histograms are obtained for blue channels of the image before embedding and extracted image. Similarly, analysis of histograms of red and green color can be done. The histogram comparisons in Figure 3 say that a histogram of the message extracted after embedding using the proposed method is closer to the histogram of the original image.

6.2. Frequency Spectrum of Cover Audio and Stego Audio. Obtaining the frequency spectrum is a universal and straightforward technique to analyze an electric signal. Figure 4 represents the snapshots of the frequency spectrum of the audio signal before and after embedding. Frequency

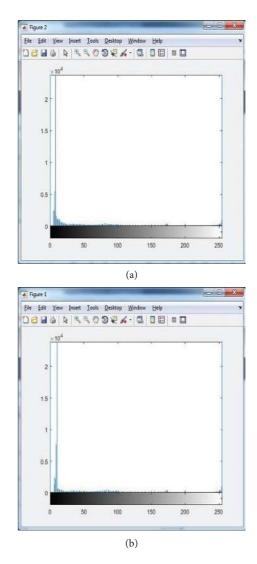


FIGURE 3: Histograms of (a) original message and (b) extracted message.

spectrums of the stego files after embedding of the secret message using the proposed algorithm and prior to embedding are obtained, and the snapshots are captured for the same interval so as to fit them on page size, as shown in Figure 4. The frequency spectrum of the stego audio is very similar to that of cover audio. Since the audio file is of long duration, the snapshots are captured for a specific time interval, as shown in Figure 4.

6.3. Analysis Using PSNR, MSE, and SSIM. PSNR, MSE, and SSIM have been widely accepted as a measure of quality. To verify the quality of the proposed method, the variation of PSNR, MSE, and SSIM values is obtained. PSNR and MSE are to calculate absolute error, but SSIM gives a measure of error in the structure.

It also looks for intensity, brightness, and other parameters that are related to the structure of an image. The unit of measuring PSNR is dB, and the acceptable value is greater than 45 dB, whereas MSE has the unit square of the unit of the quantity being measured. The desired value of

FIGURE 4: Frequency spectrum of cover audio (a) and stego audio (b).

MSE should be approaching to "0." The value of SSIM lies between "-1" and "+1." The desired value of SSIM should be approaching to "+1." "0" value indicates no similarity while value "+1" indicates that both images are identical. The results show that the improvement is significant and it would be increasing with the increase in some iteration of the proposed method. Figure 5 shows the PSNR, MSE, and SSIM variation as per the increasing iterations that reflect the significant improvement gained by using the proposed work.

6.4. Visual Inspection of Original Message and Extracted Message. The secret messages before embedding and the hidden messages extracted from stego file are compared and analyzed for any visually noticeable differences in Figure 6. The authentic recipient can easily recognize and evaluate secret message after extraction from stego audio file. The use of some reconstruction algorithm at the receiver's end may result in an identical image available for processing after extraction.

6.5. Robustness Measurement. Robustness is that property of the watermarked data that make its presence silent even after attacked with general signal processing attacks [50, 51]. The most common parameter for measuring robustness is the correlation coefficient. The higher value of correlation coefficient of original image and watermarked image is a measure of more robustness. The audio cover file with embedded watermarked is attacked with compression. The correlation coefficient was calculated after the attack for both the secret messages. The average value of correlation coefficient (Corr_{avg}) comes out to be 0.85.

6.6. Comparison with Existing Techniques. It is essential to examine and compare the efficacy of the proposed research with the preexisting techniques in a similar domain. The proposed work of optimizing audio steganography using social impact theory optimization is compared with some of the existing methods on different parameters like PSNR, MSE, and SSIM. The comparison is made using the following: (i) the traditional LSB method, (ii) another optimized steganography technique where algorithm used for optimization is GA, and (iii) the implementation work done by Chen and Huang [1].

6.6.1. Comparison of PSNR Variation. PSNR variation is compared in Figure 7, with the LSB method, with GA, and with the research work of Chen and Huang [1]. It is observed

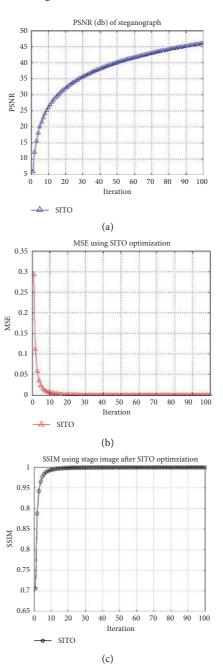


FIGURE 5: (a) PSNR, (b) MSE, and (c) SSIM variation.

from these graphs that the PSNR achieved is satisfactory while SITO is used for optimization in the proposed work.

However, the graph diverges further when the number of iterations increases. The proposed work outperforms the

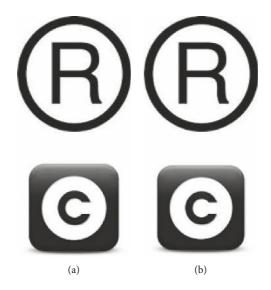


FIGURE 6: (a) Original message and (b) extracted message.

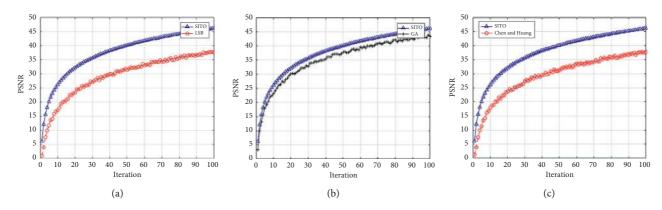


FIGURE 7: Comparison of PSNR variation with (a) LSB, (b) GA, and (c) the method of Chen and Huang [1].

LSB technique and the method of Chen and Huang [1] in case of PSNR variation. The performance greatly improves when the algorithm iterates SITO for more number of times. Figure 7 also indicates that the proposed method is far better than the LSB technique in the attainment of PSNR. Moreover, improvement in the PSNR value was observed even after few initial iterations. Similarly, GA behaves like as proposed work in initial few iterations, but after that, the variation of PSNR with respect to increase in the number of iterations starts decreasing. However, PSNR values attained by using proposed work and GA differ in the range of "0" dB to "5" dB maximum. It can be seen from the figure that the research work done by Chen and Huang [1] behave similar to the least significant bit method in the attainment of PSNR. Proposed works attain considerably greater values of PSNR as compared to the research work of Chen and Huang [1] with respect to the increase in the number of iterations.

The comparison of PSNR variation also shows that LSB technique behaved in the least effective way, while GA was comparable to the proposed method and the third one behaved in a moderate way.

6.6.2. Comparison of MSE Variation. It was observed while comparing the proposed work with the LSB method, GA, and the method of Chen and Huang [1] that GA and LSB yielded almost similar results; however, the proposed work outperformed other three techniques in this category of comparison of MSE variation.

Starting from a very high value of MSE, the proposed algorithm abruptly comes down and sooner attains the acceptance value. One more fact observed from the graphs given in Figure 8 is a little variation of MSE in all the three techniques except SITO.

6.6.3. Comparison of SSIM Variation. Structural similarity index (SSIM) is a way of measuring degradation in the quality of an image because of some processing task.

The acceptable value of SSIM should be close to one. From Figure 9, it is clear that the proposed method achieves a better value of SSIM as compared to LSB, GA, and research of Chen and Huang [1]. However, GA performs better than the other two techniques.

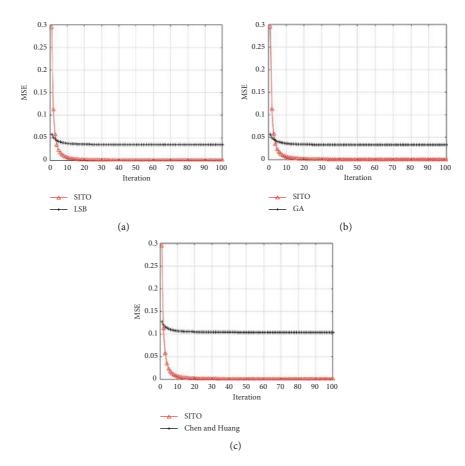


FIGURE 8: Comparison of MSE variation with (a) LSB, (b) GA, and (c) the method of Chen and Huang [1].

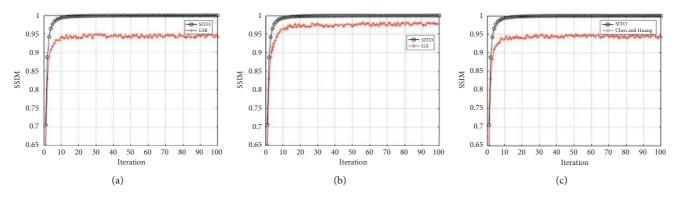
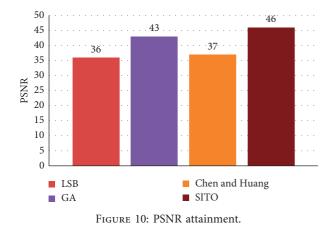


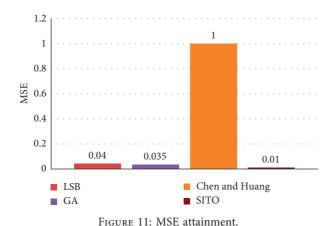
FIGURE 9: Comparison of SSIM variation with (a) LSB, (b) GA, and (c) the method of Chen and Huang [1].

6.6.4. Comparison with the Works of Su et al. [50] and Lei et al. [51]. The attainment of imperceptibility and robustness depends largely on scaling parameter chosen for embedding. Most of the audio steganography implementations use static value of the scaling parameter for simplicity. In the work done by Su et al. [50], an optimal method for the selection of scaling parameter is described that needs comparatively less computation. The optimal selection of the value of scaling parameter results in higher SNR value and larger robustness (correlation coefficient up to 0.99). On the other hand, Lei et al. [51] suggested a customized objective function and used self-adaptive particle swarm optimization technique along with quaternion wavelet transform. In their

approach, a higher value of coefficient correlation (0.99, best value) is achieved. It can be said that the optimal choice of scaling parameter in [50] and use of modified PSO in [51] outperformed the current work.

(1) Comparison of PSNR, MSE, and SSIM Value Attainment. Figures 10–12 compare the PSNR, MSE, and SSIM values achieved in each of the techniques discussed above. It is clearly deduced from the respective figures that the proposed methodology attains satisfactory and better values of PSNR, MSE, and SSIM comparatively. Genetic algorithm also performed well in attaining the evaluation parameters, but still it could not overtake the proposed work.





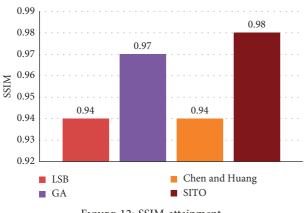


FIGURE 12: SSIM attainment.

7. Conclusion

The problem of finding an audio steganography technique with acceptable values of capacity, robustness, and imperceptibility is resolved using the proposed methodology. The characteristics of spread spectrum that makes it secure against interception and interference provide the required robustness. The prime security of steganography lies in difficulty to know the hiding pattern used for embedding. Thus, the security is ensured by making the embedding pattern truly random by utilizing chaos theory using logistic maps.

Capacity is increased by spreading a greater number of bits over the entire spectrum of a sample. This enhancement would increase the distortion too. The SITO maintains the distortion at an optimum level and optimizes the audio steganography technique to achieve the satisfactory value of the objective function. It is observed from the analysis of different graphs that significant improvement has been achieved by using social impact theory optimizer. The performance of the proposed research work improves further with the increase in the number of iterations of SITO execution. Various quality measures (PSNR, MSE, and SSIM) achieved values up to satisfaction. In some cases, GA performed somewhere close to SITO but the performance gain observed by using SITO as an optimization algorithm is more significant. The proposed methodology successfully achieves the research objectives of optimizing an audio steganography algorithm in such a way that each parameter out of robustness, capacity, and imperceptibility is attained to the satisfaction.

Data Availability

The data used to support the findings of this study are included within the article.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

References

- [1] S.-T. Chen and H.-N. Huang, "Optimization-based audio watermarking with integrated quantization embedding," Multimedia Tools and Applications, vol. 75, no. 8, pp. 4735-4751, 2016.
- [2] S. K. Pal, P. K. Saxena, and S. K. Muttoo, "The future of audio steganography," in Proceedings of the Pacific Rim Workshop on Digital Steganography 2002 (STEG'02), Kitakyushu, Japan, July 2002.
- [3] D. Sellars, "An introduction to steganography," February 2003, http://www.totse.com/en/privacy/encryption/163947. html.
- [4] S. S. Chaeikar, M. Zamani, A. B. A. Manaf, and A. M. Zeki, "PSW statistical LSB image steganalysis," Multimedia Tools and Applications, vol. 77, no. 1, pp. 805-835, 2018.
- [5] F. Arab and M. Zamani, "VW16F: a robust video watermarking using simulated block based spatial domain technique," in Proceedings of the International Conference on Security and Management, Las Vegas, USA, July 2018.
- [6] F. Arab and M. Zamani, "VW16E: a robust video watermarking technique using simulated blocks," Intelligent Systems Reference Library, vol. 115, pp. 193-221, 2017.
- [7] F. Arab, S. M. Abdullah, S. Z. M. Hashim, A. A. Manaf, and M. Zamani, "A robust video watermarking technique for the tamper detection of surveillance systems," Multimedia Tools and Applications, vol. 75, no. 18, pp. 10855-10885, 2016.
- [8] T. K. Araghi, A. B. A. Manaf, M. Zamani, and S. K. Araghi, "A survey on digital image watermarking techniques in spatial and transform domains," International Journal of Advances in Image Processing Techniques, vol. 3, no. 1, pp. 6-10, 2016.

- [9] M. Zamani and A. B. A. Manaf, "Genetic algorithm for fragile audio watermarking," *Telecommunication Systems*, vol. 59, no. 3, pp. 291–304, 2015.
- [10] M. Zamani, A. Abdul Manaf, and R. Ahmad, "Current problems of substitution technique of audio steganography," in *Proceedings of the International Conference on Artificial Intelligence and Pattern Recognition*, Orlando, USA, July 2009.
- [11] M. Zamani, A. Abdul Manaf, and R. Ahmad, "Genetic algorithm as an approach to resolve the problems of substitution techniques of audio steganography," in *Proceedings* of the International Conference on Genetic and Evolutionary Methods, Las Vegas, USA, July 2009.
- [12] M. Zamani, A. Abdul Manaf, and R. Ahmad, "Knots of substitution techniques of audio steganography," in *Proceedings of the International Conference on Telecom Technology and Applications*, Manila, Philippines, June 2009.
- [13] M. Zamani, A. Abdul Manaf, R. Ahmad, F. Jaryani, H. Taherdoost, and A. Zeki, "A secure audio steganography approach," in *Proceedings of the 4th International Conference for Internet Technology and Secured Transactions*, London, UK, November 2009.
- [14] M. Zamani, A. Abdul Manaf, R. Ahmad, A. Zeki, and S. Abdullah, "A genetic-algorithm-based approach for audio steganography," *World Academy of Science, Engineering and Technology*, vol. 30, pp. 355–358, 2009.
- [15] M. Zamani, A. Abdul Manaf, R. Ahmad, A. Zeki, and P. Magalingam, "A novel approach for audio watermarking," in *Proceedings of the Fifth International Conference on Information Assurance and Security*, Xian, China, August 2009.
- [16] M. Zamani, R. Ahmad, A. Abdul Manaf, and A. Zeki, "An approach to improve the robustness of substitution techniques of audio steganography," in *Proceedings of the International Conference on Computer Science and Information Technology*, Beijing, China, August 2009.
- [17] M. Zamani, H. Taherdoost, A. Abdul Manaf, R. Ahmad, and A. Zeki, "An artificial-intelligence-based approach for audio steganography," *MASAUM Journal of Open Problems in Science and Engineering*, vol. 1, no. 1, pp. 64–68, 2009.
- [18] M. Zamani, H. Taherdoost, A. Abdul Manaf, R. Ahmad, and A. Zeki, "Robust audio steganography via genetic algorithm," in *Proceedings of the International Conference on Information* & Communication Technologies, Karachi, Pakistan, August 2009.
- [19] S. Abdullah, A. Abdul Manaf, and M. Zamani, "Capacity and quality improvement in reversible image watermarking approach," in *Proceedings of the International Conference on Networked Computing and Advanced Information Management*, Seoul, South Korea, August 2010.
- [20] S. Abdullah, A. Abdul Manaf, and M. Zamani, "Recursive reversible image watermarking using enhancement of difference expansion techniques," *Journal of Information Security Research*, vol. 1, no. 2, pp. 64–70, 2010.
- [21] M. Zamani and A. Abdul Manaf, "Azizah's method to measure the efficiency of steganography techniques," in *Proceedings of the 2nd International Conference on Information and Multimedia Technology*, Hong Kong, China, December 2010.
- [22] M. Zamani and A. Abdul Manaf, "Mazdak's method for PSNR estimation in audio steganography," in *Proceedings of the International Conference on Computer and Computational Intelligence*, Nanning, China, December 2010.
- [23] M. Zamani, A. Abdul Manaf, R. Ahmad, F. Jaryani, S. Shojae Chaeikar, and H. Rouhani Zeidanloo, "Genetic audio watermarking," in *Communications in Computer and Information*

- [24] M. Zamani, A. Abdul Manaf, R. Ahmad et al., "Genetic audio steganography," *International Journal on Recent Trends in Engineering & Technology*, vol. 3, no. 2, pp. 89–91, 2010.
- [25] M. Zamani, A. Abdul Manaf, R. Ahmad et al., "A novel approach for genetic audio watermarking," *Journal of Information Assurance and Security*, vol. 5, no. 1, pp. 102–111, 2010.
- [26] A. Zeki, A. Abdul Manaf, and M. Zamani, "Bit-plane model: theory and implementation," in *Proceedings of the Engineering Conference*, Kuching, Malaysia, August 2010.
- [27] M. Zamani, A. B. A. Manaf, H. R. Zeidanloo, and S. S. Chaeikar, "Genetic substitution-based audio steganography for high capacity applications," *International Journal of Internet Technology and Secured Transactions*, vol. 3, no. 1, pp. 97–110, 2011.
- [28] A. M. Zeki, A. A. Manaf, A. A. Ibrahim, and M. Zamani, "A robust watermark embedding in smooth areas," *Research Journal of Information Technology*, vol. 3, no. 2, pp. 123–131, 2011.
- [29] A. Jabbar Altaay, S. Bin Sahib, and M. Zamani, "An introduction to image steganography techniques," in Proceedings of the International Conference on Advanced Computer Science Applications and Technologies, Kuala Lumpur, Malaysia, November 2012.
- [30] M. Zamani, A. Abdul Manaf, and S. Abdullah, Correlation between PSNR and Size Ratio in Audio Steganography Recent Researches in Communications, Signals and Information Technology, WSEAS, Greece, 2012.
- [31] M. Zamani, A. Abdul Manaf, and S. Abdullah, Efficient Embedding for Audio Steganography Models and Methods in Applied Sciences, WSEAS, Greece, 2012.
- [32] M. Zamani, A. Abdul Manaf, and S. Abdullah, "An overview on audio steganography techniques," *International Journal of Digital Content Technology and Its Applications*, vol. 6, no. 13, pp. 107–122, 2012.
- [33] M. Zamani, A. Abdul Manaf, S. Abdullah, and S. Shojae Chaeikar, Correlation between PSNR and Bit Per Sample Rate in Audio Steganography Recent Researches in Communications, Signals and Information Technology, WSEAS, Greece, 2012.
- [34] M. Zamani, A. Abdul Manaf, S. Abdullah, and S. Shojae Chaeikar, Mazdak Technique for PSNR Estimation in Audio Steganography Applied Mechanics and Materials, Vol. 229, Trans Tech Publications Inc., Zürich, Switzerland, 2012.
- [35] M. Zamani, A. Abdul Manaf, and R. Daruis, "Azizah technique for efficiency measurement in steganography," in *Proceedings of the 8th International Conference on Information Science and Digital Content Technology*, Jeju, South Korea, June 2012.
- [36] A. Jabbar Altaay, S. Bin Sahib, and M. Zamani, Correlation Analysis of the Four Photo Themes in Five Layers Communications in Computer and Information Science, vol. 398, pp. 211–222, Springer, Berlin, Heidelberg, Germany, 2013.
- [37] A. Jabbar Altaay, S. Bin Sahib, and M. Zamani, "Determining the threshold of pixel correlativity analysis," *International Journal of Digital Content Technology and Its Applications*, vol. 7, no. 11, pp. 164–172, 2013.
- [38] A. Jabbar Altaay, S. Bin Sahib, and M. Zamani, "Edgy photos statistical steganalysis," *Advances in Information Sciences and Service Sciences*, vol. 5, no. 16, pp. 35–48, 2013.

- [39] A. Jabbar Altaay, S. Bin Sahib, and M. Zamani, An Introduction to Watermarking Techniques Recent Advances in Electrical and Computer Engineering, WSEAS, Greece, 2013.
- [40] A. Jabbar Altaay, S. Bin Sahib, and M. Zamani, Multimedia Data Hiding Evaluation Metrics Recent Researches in Information Science and Applications, WSEAS, Greece, 2013.
- [41] A. Jabbar Altaay, S. Bin Sahib, and M. Zamani, "Partial smooth region photos statistical steganalysis," *International Journal of Information Processing and Management*, vol. 4, no. 7, pp. 130–143, 2013.
- [42] A. Jabbar Altaay, S. Bin Sahib, and M. Zamani, Pixel Correlation Behavior in Different Themes Communications in Computer and Information Science, Vol. 398, Springer, Berlin, Heidelberg, Germany, 2013.
- [43] A. Jabbar Altaay, S. Bin Sahib, and M. Zamani, "Statistical steganalysis of four photo themes before embedding," in *Proceedings of the International Conference on Advanced Computer Science Applications and Technologies*, Sarawak, Malaysia, December 2013.
- [44] A. Jabbar Altaay, S. Bin Sahib, and M. Zamani, "Wide flat region photos statistical steganalysis," *Journal of Convergence Information Technology*, vol. 8, no. 16, pp. 1–14, 2013.
- [45] A. Jabbar Altaay, S. Bin Sahib, and M. Zamani, "Wide smooth region photos statistical steganalysis," *Journal of Next Gen*eration Information Technology, vol. 4, no. 9, pp. 43–56, 2013.
- [46] R. Aghbabaeyan, S. Abdullah, and M. Zamani, "Review of digital watermarking techniques," in *Proceedings of the 1st Technology Education and Science International Conference*, Skudai, Malaysia, July 2013.
- [47] M. Salem Atoum, S. Ibrahim, G. Sulong, and M. Zamani, "A new method for audio steganography using message integrity," *Journal of Convergence Information Technology*, vol. 8, no. 14, pp. 35–44, 2013.
- [48] Z. S. Shams Dolatabadi, A. Abdul Manaf, and M. Zamani, "Using three levels DWT to increase robustness against geometrical attacks," *International Journal of Advancements in Computing Technology*, vol. 5, no. 14, pp. 86–104, 2013.
- [49] F. Tohidi, A. Abdul Manaf, M. Zamani, and H. Jamshidi, "Improving the capacity of watermarking techniques by using block truncation coding," *International Journal of Digital Content Technology and Its Applications*, vol. 7, no. 14, pp. 33–47, 2013.
- [50] Z. Su, G. Zhang, F. Yue, L. Chang, J. Jiang, and X. Yao, "SNRconstrained heuristics for optimizing the scaling parameter of robust audio watermarking," *IEEE Transactions on Multimedia*, vol. 20, no. 10, pp. 2631–2644, October 2018.
- [51] B. Lei, F. Zhou, E.-L. Tan et al., "Optimal and secure audio watermarking scheme based on self-adaptive particle swarm optimization and quaternion wavelet transform," *Signal Processing*, vol. 113, pp. 80–94, 2015.

